ABSTRACT

The invention provides a cryptographic method which includes receiving at a first entity a second public key M_A. At least one of a first session key K_B and a first secret S_B may be generated based on the second public key M_A. A first random nonce N_B may be generated which may be encrypted with at least one of the first session key K_B and the first secret S_B to obtain an encrypted random nonce. The encrypted random nonce may be transmitted from the first entity. In response to transmitting the encrypted random nonce, the first computer may receive a data signal containing a modification of the first random nonce N_B+1. If the modification of the first random nonce N_B+1 was correctly performed, then at least one of (i) opening a communication link at the first computer, and (ii) generating a first initialization vector I_B is performed.